ACCESS CONTROL PROTOCOL BETWEEN AN ELECTRONIC KEY AND AN ELECTRONIC LOCK

The present invention relates to an access control protocol between an electronic key and an electronic lock effecting logical access control.

Logical control of access to buildings, to premises containing data processing systems or systems storing assets, fiduciary, technology or information assets, is currently of great and increasing interest.

Access control methods usually employ a portable access element functioning as a key, referred to as the accessing resource, and an access resource functioning as a lock.

Logical access control between an accessed resource functioning as an electronic lock and an accessing resource functioning as an electronic key currently consists of a succession of operations to verify information or messages exchanged between the electronic key and the electronic lock.

One of the main advantages of logical access control, compared to conventional physical access control of the lock-and-key type, is the facility to allow access to an accessed resource only within a predetermined short time period.

However, if the system comprising the accessing resource and the accessed resource provides one or several accessing resources allowing access to several accessed resources through similar logical access control, counterfeiting during the validity time period of either an electronic key functioning as the accessing resource or the access control dialogue between one of the electronic keys and one of the access resources functioning as an electronic lock can then allow illegitimate access to all of the accessed resources.

Merely reproducing the logical access control dialogue between the accessing resource and one of the accessed resources allows such illegitimate access through a procedure referred to as "playback".

A conventional solution that has been implemented with the aim of responding to any such illegitimate use applies logical access control based on cryptographic mechanisms to limit the period of validity of the right of access to a short period, to foil illegitimate use outside the validity time period in the event of loss, theft or illicit holding of the electronic key. One such solution, described in French Patent Application No. 2 722 596 (94 08770) in the name of FRANCE TELECOM and LA POSTE and published 9 January 1996, establishes a digital signature of the time period during which access is authorised. Access to the accessed resource is conditional on verification of the aforementioned digital signature within the accessed resource.

Another conventional solution implemented with the same aim, more particularly to respond to playback, uses a random variable to introduce a variability or diversity characteristic into the access control dialogue between the key and the electronic lock. A solution of this kind would appear to have limitations because the random nature of the random variables obtained by means of the usual random or pseudo-random generators is not totally satisfactory unless one or more external physical variables of a purely random nature are used and because non-repetitive production of such random numbers is not certain, and will therefore not discourage highly skilled hackers who are determined to succeed and who have access to powerful computation resources.

In any event, the aforementioned solutions are therefore unable to prevent with certainty either illegitimate use of an electronic key or playback during

the validity time period of an accessed resource.

Other solutions have been proposed. Application EP-A-727 894 describes a system based on secret key cryptography. These systems raise the problem of key management as key certificates cannot easily be used. Patent application EP-A-807 911 describes a system based on secret key and public key cryptography using cyphering techniques. A public key certificate encyphered by means of a secret key is sent. The secret key used is itself sent encyphered with the public key of the recipient.

The object of the present invention is to remedy the aforementioned drawbacks of prior art solutions.

An object of this kind is achieved in particular by integrating into the logical access dialogue between an accessing resource and at least one accessed resource a process of authentication of the accessing resource by the accessed resource and making authorisation or refusal of access conditional on a successful outcome of the authentication process.

Another object of the present invention is consequently to use an access control protocol between an accessing resource consisting of an electronic key and an accessed resource consisting of an electronic lock in such a way that the authentication process is conducted in accordance with a challenge-and-response protocol and, in a particularly remarkable manner, the risk of the electronic key being compromised is further and significantly reduced to that caused by the presence in the electronic key of a simple right of access.

A final object of the present invention is to prevent all risk of picking an electronic lock by playback in a given validity time period because of the very existence of the authentication process.

The access control protocol according to the invention between an electronic key and an electronic

lock performing said access control is remarkable in that, following presentation of the electronic key to the electronic lock, the protocol consists of transmitting a random variable message prompting authentication of the electronic key from the electronic lock to the electronic key. On receiving the random variable message prompting authentication, a signature value of the random variable message prompting authentication and specific authentication data are transmitted from the electronic

key to the electronic lock, the signature value transmitted being calculated from a private signature key and the specific authentication data. After reception by the electronic lock of the signature value and the specific authentication data, the electronic lock verifies the authenticity of the signature value as a function of the specific authentication data. In response to a positive or negative result of said verification access is accepted or respectively refused.

The access control protocol in accordance with the invention between an electronic key and an electronic lock can be applied to all types of accessing resource and to all types of accessed resource.

Because the risk of playback is eliminated, calculating the signature value of the random variable message prompting authentication, making determination of that signature improbable in the absence of physical possession of the electronic key generating it, the protocol according to the present invention would appear to be particularly well suited to the secure management of a plurality of accessed resources, such as mailboxes, or even strongboxes, by means of one or more accessing resources, or electronic keys, enabling legitimate access to each of the accessed resources, the number of electronic keys being very much less than the number of mailboxes or strongboxes.

The invention will be better understood after reading the following description and referring to the accompanying drawings, in which:

- figure 1a shows a general block diagram of the access control protocol in accordance with the present invention between an electronic key and an electronic lock;

- figure 1b shows a sequential flowchart of the succession of steps for implementing the access control

protocol in accordance with the present invention between an electronic key and an electronic lock;

- figure 1c shows a preferred embodiment of a signature verification procedure used by an electronic lock (accessed resource) in accordance with the protocol according to the present invention;

- figure 1d shows one example of a mode of operation for obtaining a random variable message providing an authentication process in accordance with the protocol according to the present invention;

- figure 1e shows a procedure carried out by an electronic key for auxiliary verification of a public key enabling the electronic key to perform the random variable message signature operation in the context of the protocol according to the present invention;

- figure 1f shows one example of a method of reducing picking of an electronic lock outside at least one validity time period conforming to the protocol according to the present invention;

- figure 1g shows a particularly advantageous variant of the auxiliary verification process shown in figure 1e in which, if the electronic key has an internal clock, an additional security feature consisting of total invalidation of the electronic key is provided for situations in which access is attempted outside the validity time period;

- figure 2a shows a first advantageous variant of the protocol according to the present invention which avoids storing a second public key in each electronic lock, which increases the overall security level of the system as a whole;

- figure 2b shows a sequential flowchart of the steps of the protocol shown in figure 2a;

- figure 3a shows a block diagram of the electronic architecture of an electronic key for

implementing the access control protocol according to the present invention; and

- figure 3b shows a block diagram of the electronic architecture of an electronic lock for implementing the access control protocol according to the present invention.

An access control protocol in accordance with the present invention between an electronic key and an electronic lock providing logical access control will now be described in more detail with reference to figures 1a and 1b.

The access control protocol according to the present invention consists of a logical access control dialogue between the electronic key and at least one electronic lock, this logical access control incorporating a process of authentication of the electronic key by the electronic lock in order to authorise or refuse access. The authentication process uses message and/or data signature calculation and signature verification operations verifying the authenticity of the aforementioned messages or data.

By way of non-limiting example, the signature calculation operations followed by the signature verification operations included in the protocol according to the present invention can be based either on a secret key signature algorithm or on a public key algorithm using a private signature key associated with a public signature verification key.

The signature calculation and signature verification operations for implementing the access control method according to the present invention are described hereinafter in connection with one non-limiting preferred embodiment of the invention using an encryption or signature algorithm employing at least one public key and one private key, the algorithm being the RSA algorithm

developed by RIVEST, SHAMIR and ADLEMAN, for example. Other public key algorithms can be used without disadvantage.

Employing the usual terminology, in the context of the signature calculation and signature verification processes, if a public key algorithm is used, any signature key is a private key, which must be kept secret, whereas any signature verification key is a public key, which can be divulged. However, if a secret key algorithm is used and the secret key can be used as an encryption key to carry out a signature operation, a key of this kind and the signature verification key must be secret keys.

By convention, for any private key used to calculate a signature, the notation used for the calculation of the signature obtained by application of the private key K_S by the signature algorithm used, i.e. the RSA algorithm in the context of this example, is:

$S_{KS}(A,B,C)$

Likewise, the notation used for any signature verification operation effected by applying the public key K_P associated with the private key K_S to the aforementioned signatures or signed messages X,Y,Z, the signature being a digital message, is:

$v_{KP}(X,Y,Z)$

In any signature calculation operation, respectively signature verification operation, A,B,C, respectively X,Y,Z, designates the arguments subjected to the signature operation, respectively signature verification operation, these arguments consisting of messages or data, of course, as previously mentioned.

By definition, the verification operation using the public key K_P applied to a signature obtained by means of a private key K_S applied to an argument A and taking A as an input parameter produces a Yes/No verification

response. This verification is written:

- $v_{KP}(S_{KS}(A),A)$ = Yes/No.

If message re-establishing algorithms are used for the signature and signature verification operations, such as the RSA algorithm, a verified value VA of the argument A is obtained, and is supposedly equal to the argument A itself, of course.

To be more specific, to enable the use of the access control protocol according to the present invention, the electronic key and the electronic lock are each provided with modules Ca_k and Ca_i for calculating and memorising data, to enable storage in memory of any message necessary for the identification process, calculation of the signatures and verification of the signatures to enable use of the authentication process. The suffixes k and i represent a physical reference or address allocated to an electronic key and to an electronic lock, respectively.

In figure 1a and the subsequent figures, an electronic key EK_{kj} is used to implement the access control protocol according to the invention. The suffix k corresponds to a serial number or identifying number of the electronic key itself. The suffix j corresponds to a validation operation reference or address for the electronic key EK_{kj}, as described in more detail later. Each electronic key EK_{kj} is therefore provided with a calculation module Ca_k and a message transmission module T_k, represented by a wire antenna connected to the calculation unit Ca_k, the wire antenna enabling transmission of messages by electromagnetic means, for example.

The same applies to each electronic lock. Figure 1a shows a set of electronic locks B_1, B_i to B_N, each electronic lock B_i having a calculation and memory module Ca_i and a transmission module T_i represented by a wire

antenna and enabling electromagnetic transmission and reception of messages or data, for example.

In the event of an attempt to access a lock B_i using a key EK_{kj}, the respective wire antennas T_k and T_i are brought face-to-face to enable the exchange of messages for assuring the previously mentioned logical access control.

Generally speaking, in figure 1a, as in all the figures accompanying this description, in any general block diagram including various actors of the access control protocol according to the invention, any transaction, i.e. any exchange of messages between actors, is represented by an arrow extending from one of the actors to the other.

If an operation is effected internally, by the actors, that operation is represented by a closed arrow indicating internal execution for the actor concerned.

Finally, any transaction between two actors performed as an antecedent to implementation of the protocol according to the present invention is represented by a dashed line arrow.

The access control protocol according to the present invention between an electronic key and an electronic lock is implemented under the control of a certification authority shown diagrammatically in figure 1a and responsible for general management of the set of electronic keys EK_{kj} and the set of electronic locks B_i accessible by means of at least one of the electronic keys.

As shown in figure 1a, the certification authority can consist of a signature entity which is approved to choose and define a private key K_s in the context of execution of the signature algorithms previously referred to. The private signature key K_s is therefore chosen by the signature entity and this signature key is neither

communicated nor divulged to any other actor authorised to use the access control protocol according to the present invention.

The certification authority further comprises a validation entity which can be separate from the signature entity but is related to it hierarchically. The signature entity communicates to the validation entity the public key K_P associated with the private key K_S and authentication data DA_j which in fact consists of the signature using the private key K_S held by the certification authority of a certain number of arguments, including in particular a second public key K'_P, a time period value PH_j associated with the second public key K'_P and, for example, specific auxiliary data AUX. In the remainder of the description, the time period PH_j is referred to as the validity time period.

The second public key K'_P is associated with a private key K'_S. The initiative for choosing the second private key K'_S and the second public key K'_P can be accorded to the validation entity.

To implement the access control protocol according to the present invention, each electronic key EK_{kj} is subjected to a validation operation V_j consisting of loading and/or downloading the data parameters and messages held by the validation entity and needed to implement the access control protocol according to the present invention into the memory circuits of each of the aforementioned electronic keys EK_{kj}. The operation V_j is therefore shown in chain-dotted line in figure 1a, because it is carried out before the first use of a particular electronic key, of course. During this operation, the authentication data DA_j and the second private key K'_S are loaded into the memory circuits of each electronic key EK_{kj} and appropriate memory circuits for the data and the key are preferably provided in the

calculation unit Ca_k, the memory circuits including at least one protected memory area whose level of protection substantially corresponds to that of the protected memory areas of a smart card, for example, in order to store the second private key K'_s in a secure manner. The authentication data DA_j is specifically loaded before one or more uses of the electronic key EK_{kj}.

Thus each electronic key EK_{kj}, which is unusable before any validation operation V_j, is in fact replaced by an operational electronic key EK_{kj}, the suffix j designating the reference to the authentication data DA_j associated with the aforementioned electronic key, and in particular the validity time period of the second private key K'_s and the second public key K'_p associated with that time period.

Also, the validation operation V_j consists of loading or downloading into each key EK_{kj} the first public key K_p corresponding to the first private key K_s held by the certification authority. Specifically, the first public key K_p is loaded once only into each electronic key EK_{kj} before one or more successive uses, according to the key management policy defined by the certification authority for each application concerned.

A step V_i (figure 1a) of validating each electronic lock B_i consists of storing in memory and loading and/or downloading into the memory circuits of each calculation unit Ca_i the first and second public keys K_p, K'_p referred to previously.

After the aforementioned validation operations V_j and V_i, the access control protocol according to the present invention can be conducted between a validated electronic key EK_{kj} and any electronic lock B_i that has also been validated, as previously mentioned.

Any attempt at access by an employee holding an electronic key EK_{kj} entails that person bringing together

the respective transmission units T_k and T_i of the electronic key and the electronic lock.

This having been effected (by way of non-limiting example) between the key and the lock B_i shown in figure 1a, the electronic key EK_{kj} sends the electronic lock B_i an identification request message A_{ki}. The identification request message can be an identification number specific to the electronic key EK_{kj}, for example. Following verification of the identification request message A_{ki}, the electronic lock B_i can implement the access control protocol according to the present invention, as described hereinafter. The aforementioned verification operation can simply consist of verifying the value of the message communicated against reference values.

Referring to the aforementioned figure, the access control protocol according to the present invention consists at least of transmission from the electronic lock B_i to the electronic key EK_{kj} of a random variable message a_{ij} prompting authentication of the electronic key, after reception by the electronic lock B_i of the identification request message A_{ki} sent to it by the accessing electronic key.

Following reception by the electronic key of the random variable message a_{ij} prompting authentication, the key calculates a signature value C_i of the random variable message prompting authentication. In figure 1a, this step is denoted:

$$C_i = S_{K's}(a_{ij}).$$

Given the convention indicated, the signature value of the random variable message prompting authentication is obviously obtained from the second private key K'_s. It is clear in particular that the signature operation C_i in respect of the random variable message prompting authentication a_{ij} in fact establishes the right of access of the electronic key to the electronic lock for the true

value of that signature. It is further clear, in accordance with one particularly advantageous aspect of the protocol according to the present invention, that the right of access is modified for each transaction and each attempted access.

Following this signature calculation step, the electronic key EK_{kj} transmits to the electronic lock B_i the signature C_i and specific authentication data DA_j, the data being specific to the validity time period PH_j of the second private key K'_s and the second public key K'_p associated with that validity time period, of course. The aforementioned transmission operation is denoted C_i, DA_j in figure 1a.

Following reception by the electronic lock B_i of the signature value C_i and the specific authentication data DA_j, the electronic lock B_i verifies the authenticity of the signature value as a function of the specific authentication data, as shown by a closed arrow in figure 1a. In the same manner as previously, the aforementioned verification operation by the electronic lock B_i is denoted $v_{KPK'P}((C_i,DA_j),K_P,K'_P)$ = Yes/No.

Given the convention previously adopted, it is clear that the aforementioned verification step is effected by applying the first and second public keys K_p, K'_p, taken as parameters. The application of the aforementioned keys can also restore verified values of the random variable message transmitted by the electronic lock B_i to the electronic key and the specific authentication data DA_j. The verification operation enables the electronic lock B_i to decide to accept or refuse the requested access, according to whether they are authentic or not. Thus in the event of a positive result (Yes) of the aforementioned verification step, access is allowed whereas in the event of a negative result (No) access is refused.

A sequential description of the access control protocol according to the invention, as shown by the general block diagram in figure 1a, will now be given with reference to figure 1b.

In figure 1b, step 1000 represents the step of transmission by the electronic key EK_{kj} of the identification request message A_{ki}. That step is followed by a step 1001 representing the transmission of the random variable message a_{ij} by the electronic lock B_i to the electronic key EK_{kj}. The next step 1002 represents, based on the initial validation data V_j, and successively, the calculation of the random variable message signature C_I and transmission of the signature and the specific authentication data DA_j. The preceding step 1002 is itself followed by the step 1003, effected by the electronic lock and based on the initial validation data V_i, of verifying the authenticity of the signature value, according to the specific authentication data.

By way of non-limiting example, and for simplicity, the aforementioned verification step can generate a verification variable V, itself corresponding to a logic value 0 or 1, i.e. to the Yes or No result mentioned previously. This being the case, step 1003 is then followed by a step 1004 which is carried out at the level of the electronic lock to verify the true value of the verification logic variable V or the Yes, No result. The true value of the latter leads to authorisation of access (step 1006) whereas the absence of a true value leads to refusal of access (step 1005).

With regard to the nature of the specific authentication data DA_j transmitted by the electronic key EK_{kj} to the electronic lock B_i, as shown in figure 1a, the data consists of at least a public key certificate associated with the private signature key K'_s. The public key certificate consists of a digital signal value of at

least one validity time period PH_j relative to a right of access and the second public key K'_P.

Accordingly, given the convention previously indicated, the specific authentication data DA_j corresponds to the signature S_{KS} of various arguments such as the second public key K'_P associated with the private signature key K'_S, at least one time period PH_J associated with the second public key K'_P, the specific authentication data Da_j being obtained by application of the private signature key K_S of the signature entity. In particular, it is clear for example that various time period values can be used, for example by employing a diversity program for choosing a specific time period from among several such periods.

Note, however, that apart from the two second public key arguments K'_P and PH_j previously mentioned, another argument relating to the auxiliary data AUX can be subjected to the aforementioned signature operation S_{KS}. The auxiliary data can advantageously comprise, although this is not limiting on the invention, a serial number of the associated electronic key EK_{kj}, that serial number representing a code of the suffix k indicative of the aforementioned electronic key. Other digital values or data can be transmitted by the electronic key, by way of the field relating to the auxiliary data, as described later.

The transmission steps 1000, 1001 and the transmission substep of step 1002, as shown in figure 1b, are performed by the transmission systems of the electronic key EK_{kj} and the lock B_i, denoted by the reference T_i in the case of the lock.

Finally, in one advantageous embodiment of the access control protocol according to the present invention, the step of transmitting the electronic key EK_{kj} to the electronic lock B_i, shown in figure 1a and

referenced 1002 in figure 1b, can consist of transmitting the second public key K'_P obtained from the authentication data DA_j, for example, in addition to the signature value C_i of the random variable message prompting authentication and the authentication data DA_j. For this reason, the second public key K'_P is shown in parentheses during the transmission step shown in figure 1a and referenced 1002 in figure 1b. In a case like this, it is naturally not necessary to store the second public key K'_P in memory in the electronic lock during the operation V_i to validate each electronic lock B_i. The first public key K_P is then used during the operation of verifying the authentication data $v_{KPK'P}$ (C_i, DA_j) to attest to the authenticity of the second public key K'_P transmitted.

Generally speaking, the step of verification of the authenticity of the signature value by the electronic lock can be effected by means of a secret key when the signature calculation operation is based on that secret key or another secret key or a public key if the signature operation is based on a private key.

A more detailed description of the verification step 1003 effected by the electronic block B_i will now be given with reference to figure 1c, in the specific but non-limiting situation of using a message re-establishing algorithm such as the RSA algorithm.

As shown in the aforementioned figure, the verification step 1003 includes, in succession, a first verification step 1003a effected by the electronic lock B_i, this verification consisting of verifying the authenticity of the specific authentication data DA_j against reference data comparison criteria stored previously in the memory circuits of the electronic key EK_{kj}. It is clear in particular that applying the first public key K_P available to the signature S_{KS} provides a verified value of the public key K'_P associated with the

private signature key K'_S, given the conventions referred to above, the verified public key value denoted VK'_P, and a verified value of the time period PH_j. The auxiliary data is also reproduced when auxiliary data is transmitted by means of the argument AUX in the signature S_{KS}.

Accordingly, and in a manner that is not limiting on the invention, the reference data stored in the memory circuits of the electronic key EK_{kj} does not correspond only to the second public key K'_P associated with the private signature key K'_S, the time period value PH_j and, where applicable, the serial number of the key, which can be stored in a protect read-only circuit. The verified values following the operation of verifying the reference values can then be compared by a simple equality comparison 1003a. In step 1003a there is merely shown the equality test on the verified value of the second public key VK'_P against the stored value of the second public key K'_P.

In the event of a positive result of the aforementioned comparison in step 1003a, a second verification is performed by the electronic lock B_i in step 1003b. As shown in the aforementioned figure, this second verification consists of verifying the signature value of the random variable message prompting authentication.

Given the previous conventions, the second verification is denoted:

$$v_{K'P}(C_i) = v_{K'P}(S_{K'S}(a_{ij})).$$

Clearly during this second verification step performed in step 1003b, a verified value Va_{ij} is obtained for the random variable message prompting authentication. The verified value of the random variable message prompting authentication can then be compared with the random variable message prompting authentication a_{ij}, which will

have been stored beforehand in the memory circuits of the electronic block B_i, of course.

Thus it is clear that the second verification of the signature value is conditional on verification of the second public key K'_P associated with the private signature key K'_S and therefore, in the final analysis, on the aforementioned specific authentication data DA_j.

Generally speaking, the first verification of the authenticity of the specific authentication data, represented in step 1003a in figure 1c, can consist of checking the validity time period PH_j associated with the second public key K'_P. By applying the first public key K_P to the signature $S_{KS}(K'_P, PH_j, AUX)$, the verification step v_{KP} enables the value of the validity time period PH_j associated with the second public key K'_P to be obtained, alone, of course.

As shown in figure 1d, the random variable message prompting authentication a_{ij} mentioned above can depend on an identification value CB_i of the electronic lock. It can correspond to a serial number or a coded arbitrary number allocated to the aforementioned electronic lock B_i.

As also shown in figure 1d, the random variable message a_{ij} can also depend on a continuously increasing variable count value CO which can correspond to a date value expressed as a year Y, month M, day D, hour H, minute m and second s.

It is clear, for example, that the field CB_i and the field CO relating to the identification value of the electronic lock and to the continuously increasing variable value can be coded on the same number of bits, for example 32 or more bits, in which case each field can be combined bit-by-bit on the basis of a logical composition law $\otimes$, for example, to generate a component r_{ij} of the random variable message prompting authentication, as shown in figure 1d. The composition

law is an exclusive-OR operation, for example. The random variable message a_{ij} is then obtained by concatenating the component r_{ij} and the fields CB_i and CO. This coding method guarantees that the random variable message obtained is not repetitive.

Although the field relating to the serial number of the electronic lock CB_i can be given by any protected memory element available in the memory circuits of the aforementioned electronic lock, the count value CO can be delivered either by an incremental counter or by an internal clock available in each electronic lock. Using an incremental counter has the advantage of simplifying the circuits required to implement each electronic lock.

One particularly advantageous embodiment of the access control protocol according to the present invention between an electronic key and an electronic lock will now be described with reference to figure 1e.

Figure 1e shows the electronic key EK_{kj} as shown in figure 1a, for example. However, in addition to the calculation circuits Ca_k associated with the aforementioned electronic key, the key has an internal clock CK. The internal clock delivers a clock signal VCK to the corresponding calculation unit Ca_k.

This being so, and as shown in figure 1e, the protocol according to the present invention further consists of an auxiliary verification step 1007 for verifying authorisation of signature calculation for the random variable message prompting authentication. The auxiliary verification step is carried out by the electronic key EK_{kj} following reception of the random variable message prompting authentication a_{ij} in step 1001, as shown in figure 1a, but before the step of calculation and transmission of a signature value by the electronic key, as shown in step 1002 in the aforementioned figure.

The auxiliary verification step 1007 consists of using the first public key K_P to check the public key certificate and the validity time period PH_j associated with the aforementioned second public key K'_P against the internal clock.

Given the above conventions, and taking the second public key K'_P as a parameter, the verification operation is denoted:

- $v_{KP}(S_{KS}(K'_P, PH_j, AUX), K'_P)$ = Yes/No

However, using a message re-establishment algorithm leads to an operation denoted:

- $v_{KP}(S_{KS}(K'_P, PH_j, AUX))$

which produces the verified value VK'_P of the second public key which can be compared to the value of the second public key K'_P, as previously mentioned.

The aforementioned verification step then provides the verified value of the validity time period PH_j. The value of the clock signal VCK is compared to the validity time period PH_j to verify the validity of the second public key K'_P with which the aforementioned validity time period is associated. For example, the value of the clock signal VCK for a given validity time period can be compared to the limits which define the aforementioned validity time period PH_j.

Step 1007a is followed by a step 1007b consisting of verifying the association of the second private signature key K'_S with the second public key K'_P whose validity was verified in the preceding step 1007a. The association verification operation carried out in step 1007b can consist of calculating a signature $S_{K'S}(X)$ obtained by applying the second private signature key K'_S to a random variable X generated by the electronic key EK_{kj} (see figure 1e). A verification step applied to the verification signature value $(S_{K'S}(X)$ then constitutes the association verification step, the verification applying

to the signature calculated previously and being denoted:

$v_{K'P}(S_{K'S}(X))$.

This verification step produces a verified value VX of the random variable X in step 1007b. A test which compares the verified value VX of the random variable X with the previously stored random variable X determines the validity of the association of the second private signature key K'_S with the second public key K'_P, whose validity was verified in the preceding step 1007a.

Verifying that the validity time period PH_j is compatible with the clock signal VCK, that the verified value VK'_P of the second public key K'_P is identical to the value of the second public key K'_P, and that the verified value of the random variable VX is identical to the value of the random variable X constitutes a test which, if the result is positive (step 1007c, see figure 1e), enables the protocol according to the present invention to continue (step 1007e), which is followed by the signature of the random variable message prompting authentication a_{ij} (step 1002). In the event of a negative result, the aforementioned protocol is interrupted (step 1007d).

Performing the verification operations 1007a and 1007b using the message re-establishment signature verification algorithms, such as the RSA algorithm, previously referred to can preferably be carried out when the second public key K'_P is transmitted, in the subsequent step of transmitting the electronic key EK_{kj} to the electronic lock B_i. In any other case, in the absence of such transmission, the verification operation can be reduced to an operation of the following type, taking the second public key K'_P as parameter:

- $v_{KP}(S_{KS}(K'_P, PH_j, AUX), K'_P)$ = Yes/No

What is more, the protocol according to the present invention can be adapted to limit all attack outside of

the validity time period PH_j associated with the second public key K'_P.

To this end, as shown in figure 1f, during the step of verification by the electronic lock B_i of the authenticity of the signature value (step 1003 in figure 1a and more particularly steps 1003a and 1003b in figure 1c), following the first step 1003a of verifying the authenticity of the specific authentication data DA_j, consisting of checking the validity time period associated with the second public key K'_P, but prior to the second verification step 1003b shown in figure 1c, a plurality of tests ($1003a_1$, figure 1f) can be carried out to limit all attack outside the aforementioned validity time period. In figure 1f, the plurality of tests is represented, in a manner that is not limiting on the invention, as a comparison, within the aforementioned validity time period, of the count value CO delivered by the electronic lock B_i or, where applicable, a time signal delivered by a clock when the electronic lock has a clock. To be more specific, this test can consist of comparing the count value CO to limits defining the aforementioned validity time period PH_j, for example. If the count variable CO or the corresponding time signal is not inside the validity time period, the electronic lock B_i refuses any attempt at access. Other tests limiting attack outside the validity time period can be considered.

With regard to tests for limiting all attack outside a particular time period PH_j, a preferred non-limiting embodiment will be described hereinafter in the situation where the electronic key has a real-time clock. At the time of any attempt at access, if the verification step such as the step 1007a has been effected validly at the level of the electronic key EK_{kj}, in particular the test for the compatibility of the time variable delivered by

the clock signal VCK with the time period PH_j, the current time variable VCK delivered by the real time clock is stored in the electronic key EK_{kj}.

During the step of transmitting the electronic key EK_{kj} to the electronic lock B_i, shown in Fig.1a and referenced 1002 in Fig.1b, the time variable VCK is transmitted in addition to the signature value C_i and the authentication data DA_j, and the second public key K'_P where applicable. For this reason the time variable is shown in brackets.

The subsequent verification steps can then be performed in the electronic lock B_i.

As shown in figure 1f, for a count value CO delivered by a counter in the electronic lock B_i, a count value at the time of the attempt at access and a reference value VC_{ref} corresponding to a count value at the time of a previous attempt at access, for example, are stored in the lock.

For a time period PH_j reduced to a time interval $[VH_1, VH_2]$, it is verified that the time variable VCK stored in memory and transmitted is after VH_1 and before VH_2 and also that VCK is after VC_{ref}. If any of the foregoing verifications is not satisfied, access to the lock B_i is barred. It is accepted otherwise.

Of course, and in a manner that is not limiting on the invention, the time period PH_j can comprise a plurality of non-contiguous time intervals. In this case, the time period PH_j can be expressed in the form of a union of time intervals, in which U represents the UNION operator:

$$PH_j = [VH_1, VH_2] \cup [VH_3, VH_4] \cup \ldots \cup [VH_{n-1}, VH_n]$$

The limits which delimit each time interval can advantageously each be expressed as a date in the form day, month, year and a time in the form hour, minute, second.

To confer a very high level of security on the access control protocol according to the present invention, even more strict measures can be applied, in particular at the level of the electronic key EK_{kj}, to limit further risk of fraudulent use of the electronic key, in particular if it is lost or stolen. To this end, as shown in figure 1g, the step 1002 shown in figure 1a of calculating a signature value of the random variable message prompting authentication can be preceded by a signature authorisation auxiliary verification step, repeating some parts of the verification step 1007 shown in figure 1e, but increasing the security level of the verification by introducing a step of self-invalidation of the electronic key EK_{kj} under conditions explained below.

The electronic key EK_{kj} includes a clock CK delivering a clock signal VCK required for implementing the auxiliary verification step shown in figure 1g, in the same manner as in the case of implementing the auxiliary verification step of figure 1e.

This being so, as shown in figure 1g, the auxiliary verification step 1007 comprises a step of checking that a time variable, the clock signal VCK delivered by the real time clock CK, is inside the validity time period PH_j. Clearly, to this end, the step 1007a shown in figure 1g corresponds substantially to the step 1007a shown in figure 1e.

Likewise the step 1007b shown in both of the aforementioned figures.

In the case of figure 1g, the step 1007c of figure 1e is in fact subdivided into two sub-steps $1007c_1$ and $1007c_2$, for example.

The step $1007c_1$ consists of testing that the time variable VCK delivered by the real-time clock is inside the validity time period PH_j. If the result of the test in

step $1007c_1$ is positive, step $1007c_2$ compares the verified value VK'_P of the second public key K'_P to the value of the second public key K'_P and the verified value VX of the random variable X to the aforementioned random variable X, for example.

If the result of the test in step $1007c_1$ is negative, for example, in other words if the time variable VCK is not inside the time period PH_j, the protocol according to the present invention consists of executing a step $1007c_3$ which invalidates the electronic key EK_{kj}. The invalidation step $1007c_3$ then leads, of course, to a step 1007d of interrupting the access control protocol according to the present invention, on the grounds that the electronic key cannot be used.

Various techniques can be used to invalidate the electronic key EK_{kj}, such as short-circuiting the supply voltage of the electronic circuits, i.e. the calculation circuit Ca_k of the electronic key, and dissipating all of the electrical energy powering those circuits, or where applicable setting one or more switch-off variables for inhibiting the operation of the electronic key concerned.

On the other hand, if the result of the test in step $1007c_2$ shown in figure 1g is positive, the protocol continues (step 1007e, i.e. step 1002 of calculating the signature of the random variable prompting authentication a_{ij} as shown in figure 1a).

Variants of the access control protocol according to the present invention are naturally feasible, in particular to assure an optimum level of security, both at the level of each electronic key EK_{kj} and at the level of each electronic lock B_i.

Figure 2a shows a variant of the access control protocol according to the present invention which is particularly noteworthy in that no second public key K'_P is stored in memory in each electronic lock B_i.

To this end, firstly, the operation of validating each electronic lock B_i consists of a validation operation V_i in which only the first public key K_p is stored in the memories of the calculation units of each electronic lock B_i.

Secondly, the operation V_j of validating each electronic key EK_{kj} consists of transmitting only the specific authentication data DA_J and the second private signature key K'_s. The second private signature key K'_s is transmitted and stored in the memories of the calculation circuits Ca_k of the electronic key EK_{kj}.

During attempted access, in accordance with the protocol according to the present invention, the steps of transmitting the access request identification message A_{ki} and the random variable message prompting authentication a_{ij} from the electronic lock B_i to the electronic key EK_{kj} are unchanged.

On the other hand, the step 1002 previously described of calculating the signature value of the random variable message prompting authentication a_{ij} is modified in the following manner. The authentication data is verified first, this verification being denoted $v_{KP}(S_{KS}(K'_P, PH_j, AUX))$.

With the preceding convention, the second public key K'_P is restored, which enables the signature value $C_i = S_{K'S}(a_{ij})$ of the random variable message to be calculated on the basis of the available second private signature key K'_s. Because the signature value is available and stored in memory, the operation of transmitting the signature C_i of the random variable message prompting authentication, the specific authentication data DA_j and the second public key K'_P to the lock B_i can be carried out.

The protocol according to the present invention is then resumed at step 1003 of figure 1a for example by the

lock B_i.

All the verification steps, followed by the steps of calculating the signature values C_i, followed by the aforementioned transmission, are represented in steps 1002a, 1002b, 1002c of figure 2b, prior to execution of the step 1003 previously mentioned.

There follows a description with reference to Figures 3a and 3b of the architecture of an electronic key and an electronic lock for implementing the access control protocol according to the present invention.

Figure 3a shows an electronic key EK_{kj} which has a cryptographic calculation module Ca_k, a message or data transmission module E_k and a transmit/receive wire antenna T_k, as previously described. The cryptographic calculation module comprises, in addition to a central processor unit CPU, a protected access memory area 1 for storing at least one signature value of a validity time period allocated to the electronic key, that signature value corresponding of course to the specific authentication data DA_j previously mentioned. The protected access memory area 1 is also used to store a signature verification key, the first public key K_p, i.e. the aforementioned signature, consisting of the specific authentication data. It also stores a signature key, the second signature key K'_s mentioned previously. This embodiment corresponds to the embodiment of the protocol according to the present invention shown in figure 1a.

The cryptographic calculation model Ca_k also includes a read-only memory (ROM) 2 enabling the central processor unit CPU to call programs for calculating the signature value of a random variable message, i.e. the message a_{ij} previously mentioned, and for signature verification on the basis of the signature keys, respectively signature verification keys, i.e. the keys K'_s and K_p previously mentioned. The read-only memory 2 of

the key stores programs for calculating signature values of the random variable message and verifying signatures on the basis of the signature keys K'_s and signature verification keys K_p, K'_p, as in the flowcharts shown in figures 1e and 1g previously described.

In addition to the above, and depending on the embodiment of the protocol according to the present invention used, the cryptographic calculation module Ca_k includes a clock 3, for example, delivering the clock signal VCK to the central processor unit CPU and, of course, a scratchpad random access memory (RAM) 4.

Finally, the system has a serial port PS for implementing the validation step V_j previously mentioned.

With regard to the electronic lock B_i shown in figure 3b, it has, of course, a cryptographic calculation module Ca_i and a message transmission/reception module E_i both associated with an antenna T_i which is shown as a wire antenna in figure 3b, without this being limiting on the invention.

The cryptographic calculation module Ca_i includes a protected access memory area in addition to a central processor unit CPU. The protected access memory area is used to store at least one public signature verification key, i.e. the first public key K_p and the second public key K'_p in the embodiment of the protocol according to the present invention shown in figure 1a, or respectively to store a single public key, i.e. the first public key K'_p in the embodiment of the protocol according to the present invention shown in figures 2a and 2b.

What is more, a read-only memory 6 connected to the central processor unit enables the central processor unit to call signature verification programs based on the public key or keys K_p, K'_p previously mentioned. The read-only memory 6 stores signature verification programs, for example, whose flowchart corresponds to that shown in

figures 1d, 1c and 1f previously described. Similarly, a counter 7 or if necessary a real-time clock and a serial port PS are provided.

An access control protocol between an electronic key and an electronic lock has therefore been described, the electronic lock applying access control in a particularly powerful manner in that the electronic key, which has cryptographic potential, is able to authenticate its attempt to access each of the accessed electronic locks.

A protocol of the above kind would appear to be of major benefit because the operation of signature by the key of the random variable message prompting authentication constitutes a variable right of access, changing on each transaction, so that playback is prevented.

Finally, the protocol according to the present invention can be used to optimise the overall security level in that a single signature verification public key can be stored in each electronic lock. It constitutes a secure method of access control. The optimisation is adapted to suit the application.

The protocol according to the present invention and the electronic key and the electronic lock for implementing the protocol would appear to be particularly suitable for management by approved employees of strongboxes or mailboxes, for example.